Improving Reliability for Power System Protection

S. Ward T. Dahlin W. Higinbotham

RFL Electronics Inc

353 Powerville Road

Boonton Twp, NJ 07005

Presented to the

58th Annual Protective Relay Conference
Atlanta, GA
April 28 - 30, 2004

Improving Reliability for Power System Protection

S. Ward T. Dahlin W. Higinbotham

RFL Electronics Inc

353 Powerville Road

Boonton Twp, NJ 07005

Abstract

Reliability is always a concern for protective relay systems. Reliability is a compromise between security and dependability. Security is the ability to properly restrain from tripping when not called for. Dependability is the ability to trip when required. While security is not improved by increased redundancy, dependability is. Clearly, the impact on the power system when a protection device is not functioning when required is much less severe when there is a redundant device that takes over the job. If the two redundant devices are of equal performance, there should be no detrimental effect at all on power system operations, and a non-functioning device would just need to be repaired or replaced.

The telecoms industry applies a “no single point of failure” criteria for communications networks. Reliability is commonly achieved by configuring the communications links in rings. A ring provides an alternative communications path rather than a duplicated communications cable, minimizing capital investment costs and still satisfying reliability requirements.

For relaying, the preferred method of meeting reliability requirements has been to use physically separate, redundant protection devices. A pilot protection scheme consists of relays, communications interface device and a communications channel. All of these need to function properly for the protection scheme to operate as intended. The reliability of a pilot protection scheme, even with a channel independent Zone 1, would benefit as much from redundant communication channels as redundant relay devices. However, independent channels are not always economically justified due to the high cost involved for a second communications link.

This paper is examining redundancy requirements for relaying and presents a new approach. The paper suggests that a single device with redundant modules can accomplish as high, or higher, redundancy as the physically separate box concept. The paper also presents practical, affordable means of realizing redundant communications channels.

Reliability

Reliability is a product of two factors; dependability and security. For relay system protection, dependability is defined as the ability to trip for a fault within its protective zone while security is the ability to refrain from tripping when there is no fault in the protective zone.

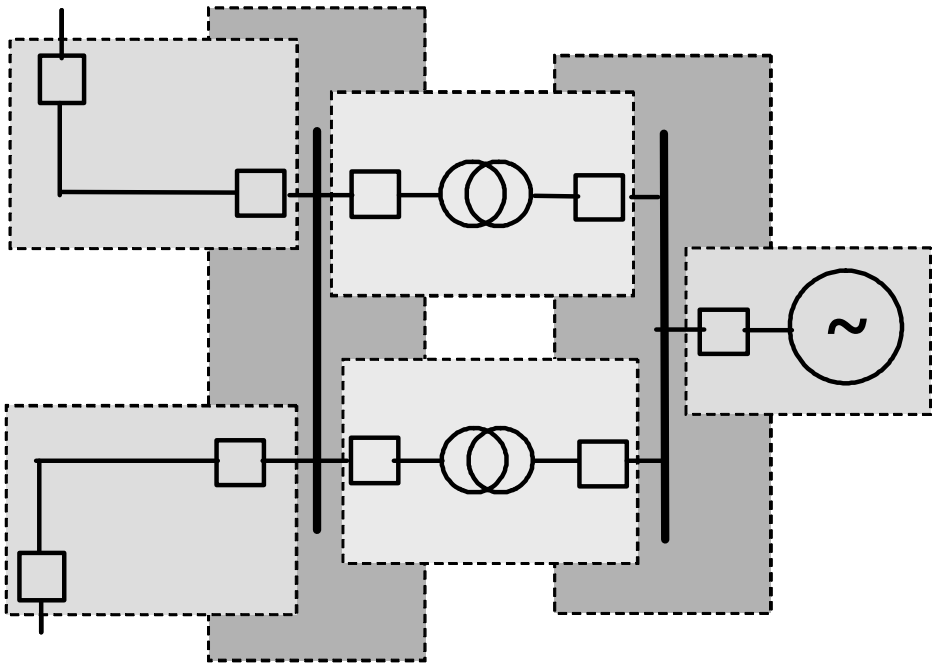

Figure 1. Zones of Protection

While not practical to use, it could be of interest to illustrate the concepts by looking at the two extremes; 100% dependability and 100% security. 100% dependability would be achieved by a protection system that is in constantly tripped state, hence there is no possibility that there would be a fault that would not be detected. 100% security would be achieved by disabling the protection system entirely so that it could not trip. From this we can see that while high dependability and high security are desirable, they will both have to be less than 100%. Generally, an increase in dependability will decrease security, and vice versa. However, measures to increase dependability may not penalize security to an equal degree and the aim of a protection system design is to find the optimum combination of the two factors in order to provide adequate reliability of the protection system.

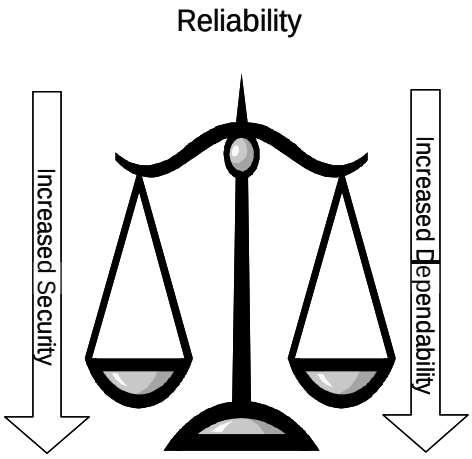

Figure 2. Reliability, dependability and security

Dependability

For a protection system, dependability is easy to define and to measure. Any in-zone fault that is not tripped by the protection is considered lack-of-dependability. The reciprocal of dependability could be called 'failure to trip'. For example, if a system has a dependability of 99%, the failure to trip would be 1% which means that of 1 out of 100 faults in the protected zone would not be tripped by the scheme.

Security

Security is the ability not to trip when not called for. To put a number on security is not as easy as for dependability. A simple method would be to compare the number of false trips for faults external to the protected zone as compared to the total number of external faults. However, this does not consider other phenomena; false trips due to relay failure, trips on stable power swings, inrush currents or other phenomena that are not necessarily classified as power system faults. Even an 'external fault' is not readily defined as it depends on what extent of the adjacent power system is included in the fault count.

A practical approach to determine security was made by the 'Transmission Protective Relay System Performance Measuring Methodology IEEE/PSRC Working Group I3' [2]. The Working Group suggests to measure security as the number of false trips relative to the total number of events recorded during a time period. While this does not provide a security estimate according to the strict definition of security it certainly is a useful measurement for protective relay system performance comparisons.

Redundancy

Redundancy is defined as 'the existence of more that one means for performing a given function' [1]. It is obvious that protective relay system dependability can be increased by added redundancy as if one of the systems does not trip for an in-zone fault, a redundant system may. Security on the other hand, is generally decreased by increased redundancy as there are added devices in the system that may trip when not called upon to do so. However, redundancy does not influence dependability and security to the same degree.

In order to illustrate how redundancy influences dependability and security, data is borrowed from a teleprotection standard, IEC 60834-1. To our knowledge, no such standard exists for relays. The IEEE/PSRC report referenced above does not directly address redundancy. If a fault occurs and is isolated from a backup (or redundant) protective system, the fact that the primary relay system did not operate does not constitute a mis-operation. The reason for this is obvious; as long as the fault is correctly tripped, there is no reason to investigate whether all parts in the protective relay system actually operated as intended.

The IEC 60834-1 (1999) 'Teleprotection equipment of power systems – Performance and testing' [3] does not only specify security and dependability requirements but also how these are determined by testing. Security for teleprotection is measured as the number of false trips for a given number of 'noise bursts' or bit-errors on the communication channel. Dependability is measured as the number of missed commands for a given number of 'noise bursts' or bit-errors on the communication channel. While not easily translated into something relevant to a stand-

alone relay, they can be used to illustrate the influence of redundancy on dependability and security.

In the following discussions, 'redundant' refers to completely independent systems or components. The failure rate for each system or component is independent from the redundant system's failure rate. A failure in one device does not influence the other and the failures are not triggered by a common cause.

For our redundancy considerations, the requirements given for a Direct Transfer Trip Teleprotection System are used:

- 99.9999% security
- or expressed as probability of a false trip (reciprocal of security)
  - 10^{-6} or 1/1,000,000
- 99.99% dependability
- or expressed probability of a missed trip (reciprocal of dependability)
  - 10^{-4} or 1/10,000

Security in a redundant system

If we add a redundant system, and the systems are equal and independent, the probability of a false trip will be the sum of the probability for each redundant system to give a false trip:

- Probability of a false trip for a redundant system = 2/1,000,000
- or expressed as security: 99.9998%

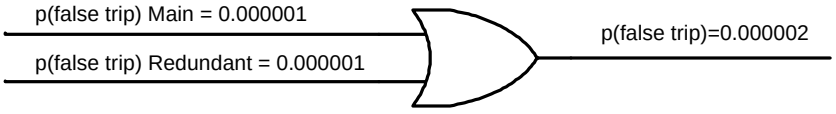

Figure 3. Probability for false trip in a redundant system

Security is reduced from 99.9999% for a single system to 99.9998% for a redundant system, which is not a significant change.

Dependability in a redundant system

The probability of a missed trip however, will be greatly reduced, resulting in much improved dependability. If the systems are equal and independent, both of them need to fail at the same time for a missed trip to occur. Therefore the resulting probability of a missed trip is the product of the individual probability:

- Probability of a missed trip for a redundant system = 1/10,000 x 1/10,000 = 1/100,000,000
- or expressed as dependability: 99.999999%

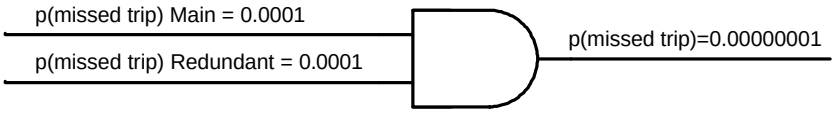

Figure 4. Probability for a missed trip in a redundant system

Consequently, dependability has increased from 99.99% to 99.999999%.

Influence of redundancy on security and dependability

The table below summarizes the influence of redundancy on security and dependability for the example used with individual unit probability of a false trip of 10^{-6} and probability of a missed trip of 10^{-4}.

Scheme	*Probability of a false trip*	*Security*	*Probability of a missed trip*	*Dependability*
Single	10^{-6}	99.9999%	10^{-4}	99.99%
Redundant	2×10^{-6}	99.9998%	10^{-8}	99.999999%

Table 1.

The above example hopefully explains why redundancy is important for protective relay system reliability. By adding a second redundant system the probability of a false trip increased by a factor of 2, but the probability of a missed trip decreased by a factor of 10,000.

Reliability of multi-function protective relays

Most new relay installations are made with multi-function microprocessor relays. As compared to conventional electromechanical relays, these devices offer greatly increased *functional* redundancy, but often a decrease in *hardware* redundancy. A main protection multi-functional device often includes a large number of back-up functions in addition to the main protection algorithm. Sometimes these functions would be replacements for conventional back-up devices but more often provide added back-up or redundant functionality as compared to the original protection system, just because they happen to be available ‘free-of-charge’. While the probability of hardware device failures causing false trips has not been increased, the probability of false trips due to incorrect settings or improper application would increase with each function used.

Reliability of a protective relay system

The relay is just one component that needs to function correctly for the protective relay system to operate as intended. Other components are: circuit breakers, measuring transformers, battery system, control circuits, teleprotection devices and any communications channels. While it is of interest to examine the performance of all these components, this paper will discuss only relay and teleprotection aspects of protective relay system reliability.

Misoperations caused by relay and teleprotection devices can have many causes:

- Equipment hardware failure
- Relay measuring limitations
- Software defects
- Incorrect settings or improper application
- Control wiring problems

Redundancy can improve each of these factors, but in different ways:

Equipment hardware failure

The use of redundant protection systems will greatly improve dependability for equipment failures. Simple means such as redundant power supplies connected to independent battery systems are also useful.

Security could be adversely affected by added redundancy, but the likelihood is small. There is a risk that a hardware failure could cause a false trip before being taken out-of-service by the self-supervision, but this is not a very common occurrence.

For hardware failures, the choice of identical or different redundant systems would make little difference. Exceptions would be if there is a common mode failure or a design flaw that would be affected by common external factors.

Relay measuring limitations

Redundancy will not improve dependability for relay measuring limitations unless they are of different design, or at least use different settings, eliminating the possibility of identical limitations in both devices. This fact has influenced the practice of applying different measuring principles, and/or designs, for the Main 1 and Main 2 protection schemes. Recognizing that it might be difficult to design a protection scheme that would cover all conceivable system fault conditions, it has been common to apply two schemes to complement each other. As correct fault clearing requires just one main protection to operate properly, this practice has proved to be very effective.

Security will be adversely affected by added redundancy, and the resulting probability of false trips will be the sum of the probability of false tripping for all individual devices connected in parallel. There has been some attempts to improve this situation by, for instance, applying two-out-of-three tripping schemes. This means that three main protection systems would be used and to trip the breaker two of these three schemes would need to make a trip decision. This will provide the dependability of a dual redundant scheme for internal faults and at the same time keep security high as any one false relay operation will not cause a false trip.

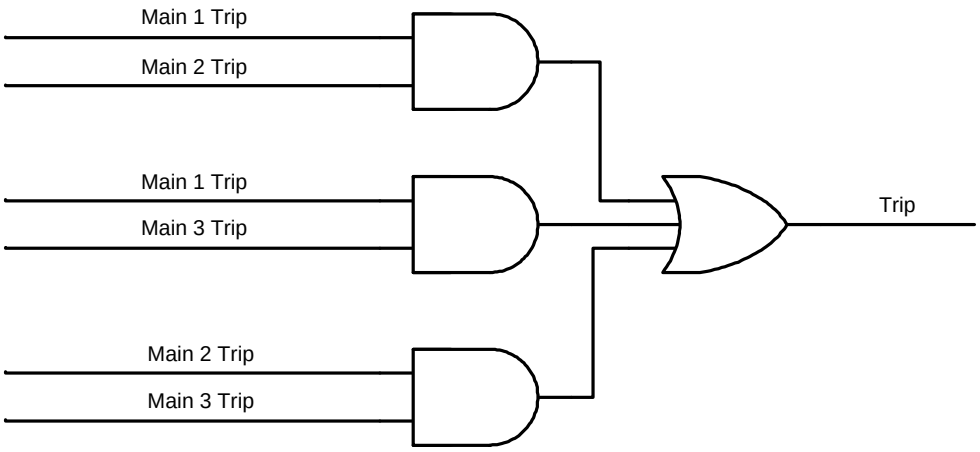

Figure 5. Two-out-of-three trip logic

We can estimate the resulting improvement in security and dependability for the two-out-of-three scheme by applying the same principles as used for the dual scheme previously.

Security for the two-out-of-three scheme

For a false trip, two protections need to misoperate at the same time. Consequently, the probability of a false trip is the product of the probability of false trip for the individual schemes. Assuming that they are equal, independent and using the 10^{-6} figure, the combined probability for a false trip is 10^{-12}.

Dependability for the two-out-of-three scheme

For a missed trip, two of the three relays need to fail to operate for an in-zone fault. This means that the dependability is exactly the same as for a redundant system with two relays, assuming that they have equal and independent probability of a missed trip. Using the 10^{-4} figure from earlier, the combined probability of a missed trip is 10^{-8}.

Two-out-of-three compared to redundant system

Based on the example using a probability of false trip of 10^{-6} and probability of missed trip 10^{-4}, the two-out-of-three configuration compares to a dual redundant scheme as follows:

Scheme	*Probability of a false trip*	*Probability of a missed trip*
Two-out-of-three	10^{-12}	10^{-8}
Redundant system	2×10^{-6}	10^{-8}

Table 2.

The two-out-of-three configuration shows an equal improvement of dependability and a considerable increase in security as compared to the redundant scheme using two protections only. However, this increase in security may not justify the extra cost of one more protection scheme.

Software defects

While software defects in protection devices may be rare as compared to other computer equipment, they still do occur. With the increased complexity of multi-functional devices there are an infinite number of configurations and setting combinations that should be tested. It seems inevitable that some defects will go undetected until the device is in service. False trips may consequently occur due to software defects and this is possibly the least popular type of nuisance trips. Unfortunately, redundancy will only make the situation worse. Redundant devices and/or functions may improve dependability but more notable is the loss of security. Every device or function added to the scheme will add to the probability of false trips.

Incorrect settings or improper application

Incorrect settings and improper application will affect both dependability and security. A redundant device or function will improve dependability but it will also decrease security. The large number of additional functions available in the multi-function devices may have a greater negative impact on security than the relatively marginal improvement in dependability. Many of these functions are for back-up and are rarely called on to operate, but an incorrect setting may cause a false trip. In addition, the large number of functions to be set and tested by the protection engineer has increased the possibility for human error.

Control wiring problems

Control wiring problems can be divided into different categories; battery, measuring transformer, breaker trip and communication circuits. Some of these can be made redundant while others may be too costly to consider. For instance, a circuit breaker can be equipped with two, redundant, trip coils but the circuit breaker itself is not duplicated. A second communication channel will greatly improve protection scheme dependability but may be difficult to realize.

Adding redundancy in the protection equipment itself can improve dependability for control wiring. Examples are:

- Redundant power supplies fed from different battery systems
- Redundant trip outputs operating on different trip coils
- Redundant digital input boards
- Redundant comms interfaces
- Main 1 and Main 2 protections connected to different measuring transformers or different secondary windings

Protection System Redundancy

The most common protection philosophy is to use two physically separate Main 1 and Main 2 relay systems (or a Primary and Backup system) for redundancy. Redundancy is also applied for other critical parts in the protection system chain when economically feasible:

- Dual trip coils are commonly used, either with Main 1 and Main 2 operating on separate trip coils, or cross connected so that both relays trip both coils.
- Redundant station battery systems are common but few relays are supplied with redundant battery supplies so that failure of one battery system may take one of the protections out-of-service.

- Common or separate measuring transformer cores are used, depending on availability.
- Redundant pilot communication channels may be used when available. The use of one common channel for two redundant relay schemes is also applied. Less common is the use of two redundant channels for one relay scheme.
- Back-up relaying such as breaker failure protection used to be a separate device but is increasingly being included in the main protection scheme, or in both main protection schemes.
- A communications channel for a main protection is given double duty to also transfer Direct Transfer Trip and control commands that earlier used separate communication links. This decrease in redundancy is often compensated by adding a second main protection communications link, where previously only the Primary protection was a pilot scheme.

Microprocessor Relay Hardware Design

Examining a typical multi-function microprocessor relay, we find a number of typical 'main' component blocks:

- Power supply
- Input transformers with A/D converters
- Opto-coupler inputs
- Relay or solid state outputs
- Microprocessor board
- HMI and display/front panel processor baord

Depending on the design, these component blocks may have been combined on one physical board, or they may each have their own board or module. Typically, this type of device does not provide much hardware redundancy, with the exception of optional dual power supplies and optional redundant pilot communication interfaces.

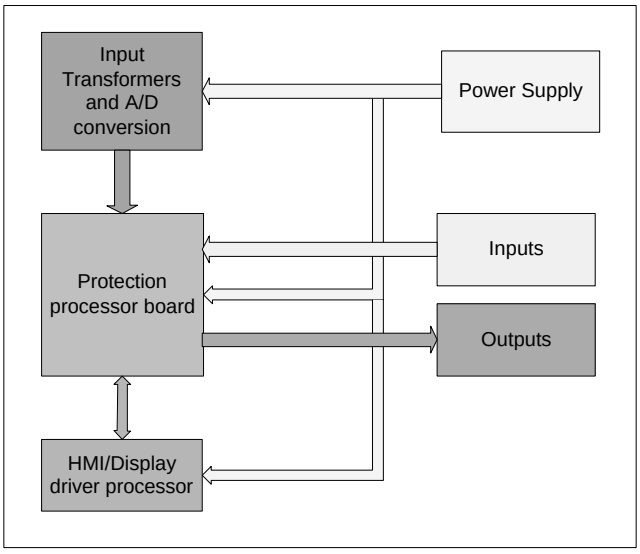

Figure 6. Microprocessor relay hardware blocks

All of these component blocks need to be functional at all times for proper relay operation. Consequently, the total failure rate is the sum of the failure rates for each component block.

The failure rates below are based on part counts. A parts count is a theoretical evaluation of the individual component block adding up failure rates for each component in the block. A part count provides a very pessimistic figure as it does not take into account design quality or component failures that are detected before delivery during production tests and burn-in processes. However, for comparison purposes, it is of little importance if the actual figure is lower, as we assume that the relative relationship between the component blocks remain the same.

The part counts in Table 3 are based on MTBF (Mean Time Between Failure) calculations using Bellcore Calculation Method 5. The MTBF results can then be converted for failure rates according to the formula:

$$\text{Failure rate} = \text{Number of failures per year} \cong \frac{1}{\text{MTBF (in years)}}$$

Unit	*Failure rate as per part count*
Power supply	0.008
Input unit	0.005
Output unit	0.005
Main processor block	0.011
HMI processor block	0.006
Input transformers and A/D conversion	0.010
Total failure rate for one device	**0.045**

Table 3.

While the failure rate is not identical to lack-of-dependability (not all failures will necessarily cause a missed trip) we can assume that most of them will result in the relay not being operational. For simplicity, the following discussion assumes that failure rate equals lack-of-dependability, and that each failure will result in failure to trip.

When adding a second, independent, redundant system, the resulting probability of failure to trip of the combined system is the product of the failure rates of the individual systems:

Failure rate for a redundant system = 0.045 x 0.045 = 0.002

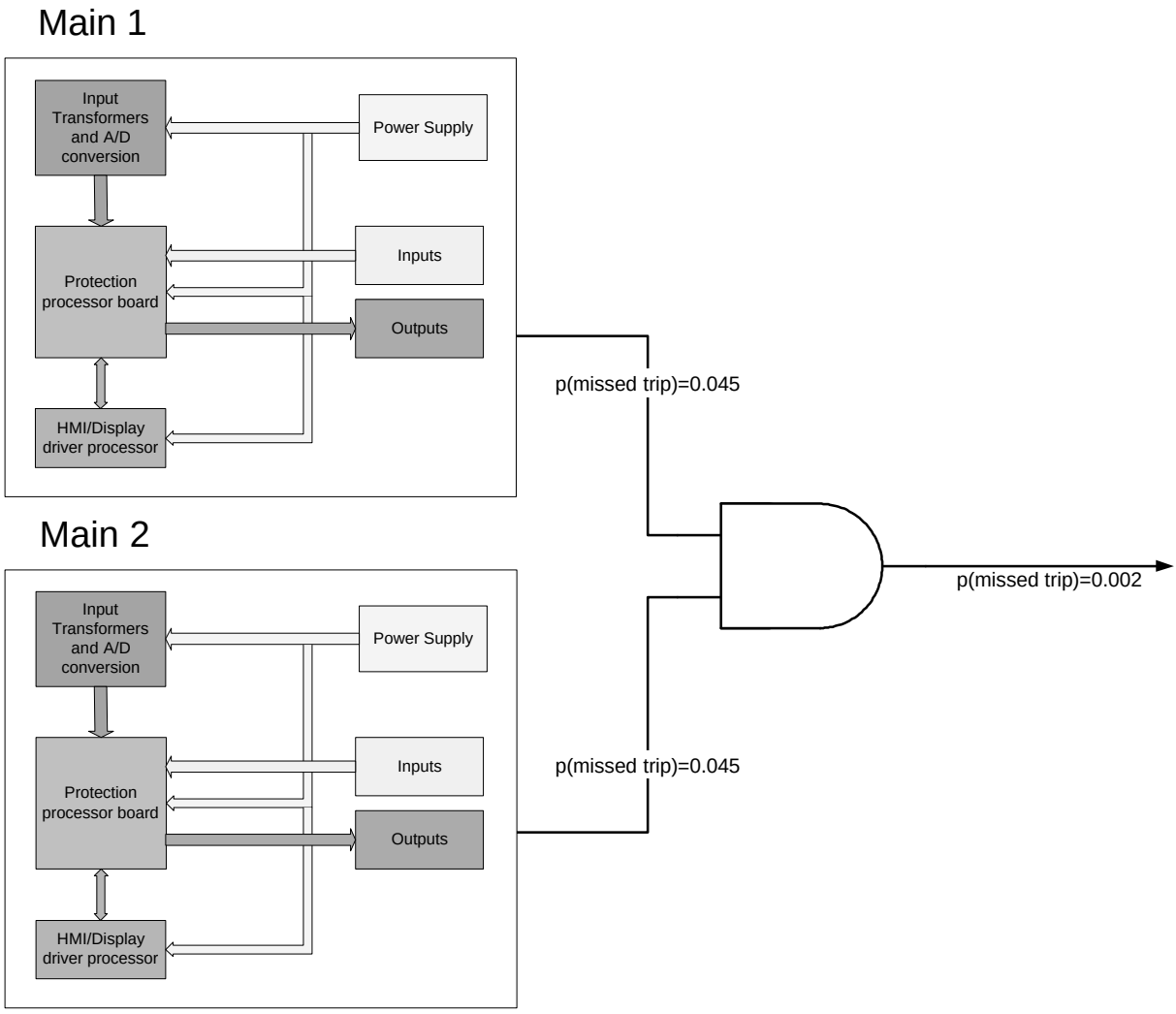

Figure 7. Redundant relay system

Translating failure rates back into MTBF, we can see that the redundant system's MTBF is 500 years as compared to the single system's MTBF of 22 years.

The results are summarized in Table 4.

System	*Failure Rate (failures per year)*	*MTBF (years)*
Single system	0.045	22
Redundant system	0.002	500

Table 4.

A new approach to redundancy

Protective relay system redundancy is conventionally achieved by adding another, redundant, relay system. In a related field, telecoms industry, redundancy requirements are met not with physically separate boxes, but rather with redundant functional modules within the same system. Clearly, this trend is driven by cost restrictions as it is less costly to add a module than to add an entire system. However, does this mean that the telecoms industry accept less reliability than what is required for protective relaying?

We determined above that the failure rate for a system based on two separate, redundant relays was 0.002 failures per year, or an MTBF of 500 years. We will do the same evaluation for the new redundant configuration:

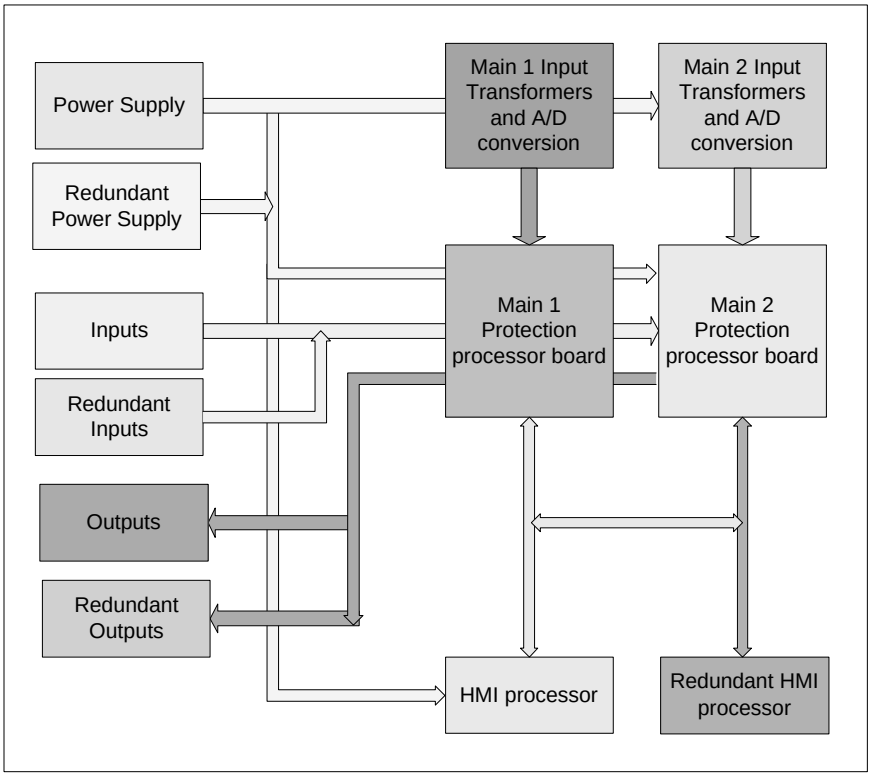

Figure 8. New redundant relay system

This system is built up of redundant modules on each level. Each protection block has access to redundant power supplies, redundant inputs, redundant outputs and redundant HMI processor boards. As these redundant modules are shared with the redundant protection blocks, the solution is cost efficient while providing a very high degree of reliability for hardware failures. We can estimate the failure rate for this redundant system:

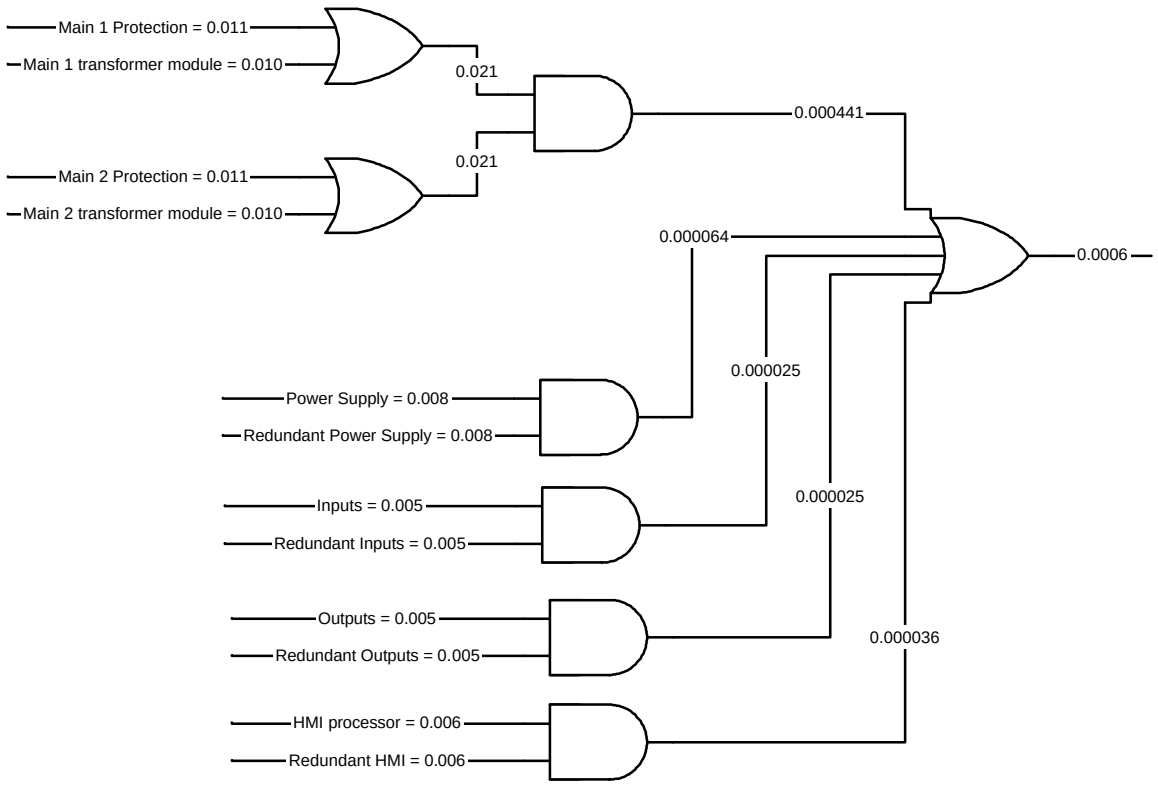

Figure 9. Failure rate for the new redundant system

The failure rate estimation has been made by use of a 'Fault Tree' [4]. An AND gate represents the probability that both modules fail at the same time for the output to fail. An OR gate represents that if any module connected to this gate fails, the output will fail. Consequently, the failure rate for an AND gate is the product of the inputs while the failure rate of an OR gate is the sum of the inputs. All redundant modules in the system are connected via AND gates, and the outputs of these are finally combined in an OR gate. The redundant Protection modules comprise both the input transformer circuitry and the microprocessor module. These two modules are therefore combined in an OR gate before entering the Protection AND gate.

The resulting failure rate for our new redundant system is 0.0006, or an MTBF of 1667 years, which is significantly higher than a conventional redundant system.

Failure rates for the new redundant system, a conventional redundant system and a single system

Our calculations are summarized in Table 5 for the three systems examined:

System	*Failure Rate (failures per year)*	*MTBF (years)*
Single system	0.045	22
Conventional redundant system	0.002	500
New redundant system	0.0006	1667

Table 5.

An observant reader might object that there are common parts in the ‘new redundant system’ that have not been taken into account for the failure rate; the chassis itself and ‘backplane’ (that for this system actually is a mid-plane). This is true but the reason is that the failure rates for these passive devices are negligible. The chassis is a metallic structure without any components. The mid-plane, on the other hand, has connectors that could fail. This failure rate has been added to the failure rate for the module using the connector, and has therefore been considered in the total failure rate count.

Redundancy for protective relay and teleprotection devices

The relay communications channel is an important part of the protective relay system. It could be argued that with a distance relay, Zone 1 would still provide protection independent of any communications channel. However, for correct high-speed tripping and resulting success of reclosing, an operating communications link is required. Commonly, automatic reclosing is disabled in case the communications channel is not functional. Consequently, a line fault, whether permanent or not, will result in the line being taken out-of-service until closed by other means. Also, in case of a sequential trip (zone 1 at one line end and time-delayed zone 2 at the other) there is a much increased risk of trips by adjacent back-up functions.

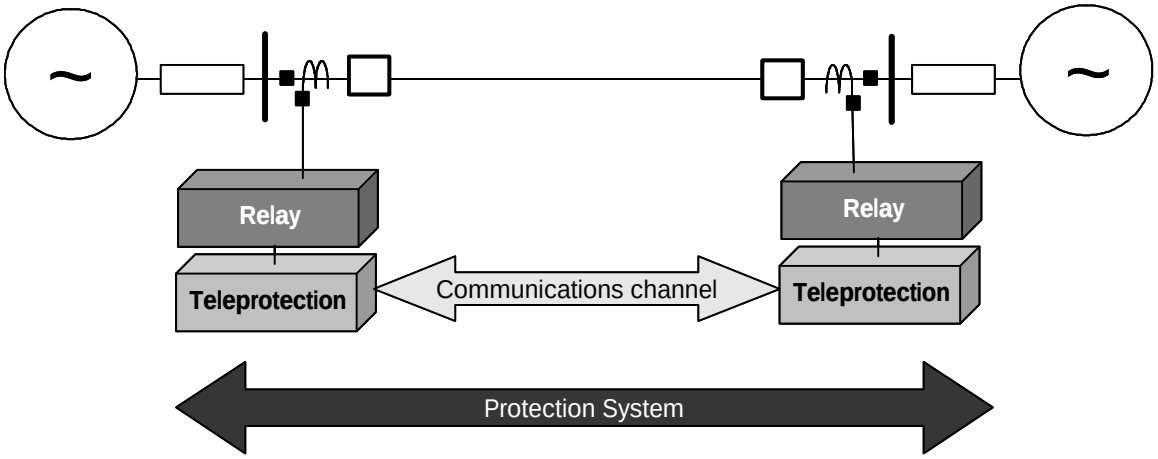

Figure 10. Protective relay system.

To evaluate redundant protection systems, including redundant communications channels, we will reuse the failure rates for the relays used in the examples above. Considering that many relays today have built-in communications interfaces, we will add only the failure rate for this interface to the total rate for a pilot protection scheme. A typical failure rate for a fiber optic communications interface, such as used for single mode dedicated fiber, is 0.024. The failure rate for the dedicated fiber itself is ignored in our calculations as this component is external to the relay system devices and will be equal for the different redundancy configurations presented.

Single relay, single channel

The failure rate for a pilot protection scheme comprising one relay and one communications channel is the sum of the failure rates for the relay and the comms interface as shown in Table 6. For a line protection, the equipment at both line ends need to be functional, which is shown in column 3 in the table.

System	*Failure rate per terminal (failures per year)*	*Failure rate per line protection (two terminals)*	*MTBF (years)*
Relay	0.045	0.090	11
Communications interface	0.024	0.048	21
Relay and comms interface	0.069	0.138	7

Table 6.

Redundant relays, redundant channels

Adding a redundant channel to redundant relays will result in a high degree of improvement as compared to a single relay, single channel system. For a conventional relay system, the redundancy is achieved by adding one more complete relay and comms channel. In the example we are using, each relay has a direct fiber comms interface and there consequently need to be two fiber pairs available for communications between the two line ends.

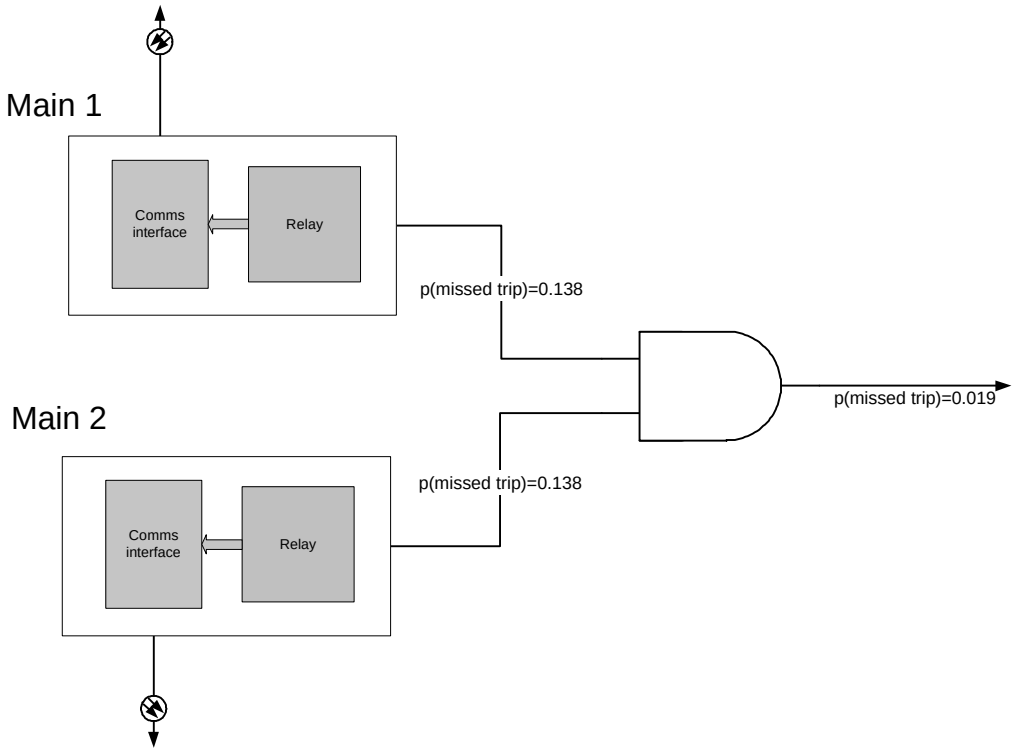

Figure 11. Conventional redundant relay and redundant channel system

Table 7 summarizes the comparison between a single relay, single channel system and a redundant relay, redundant channel system.

System	*Failure rate per line protection (two terminals)*	*MTBF (years)*
Single relay with single channels	0.138	7
Redundant relay with redundant channel	0.019	53

Table 7.

New redundant system with communications

The new redundant relay system presented earlier can also incorporate comms interfaces. We can use the same redundancy principle by making each comms module available to both protection modules.

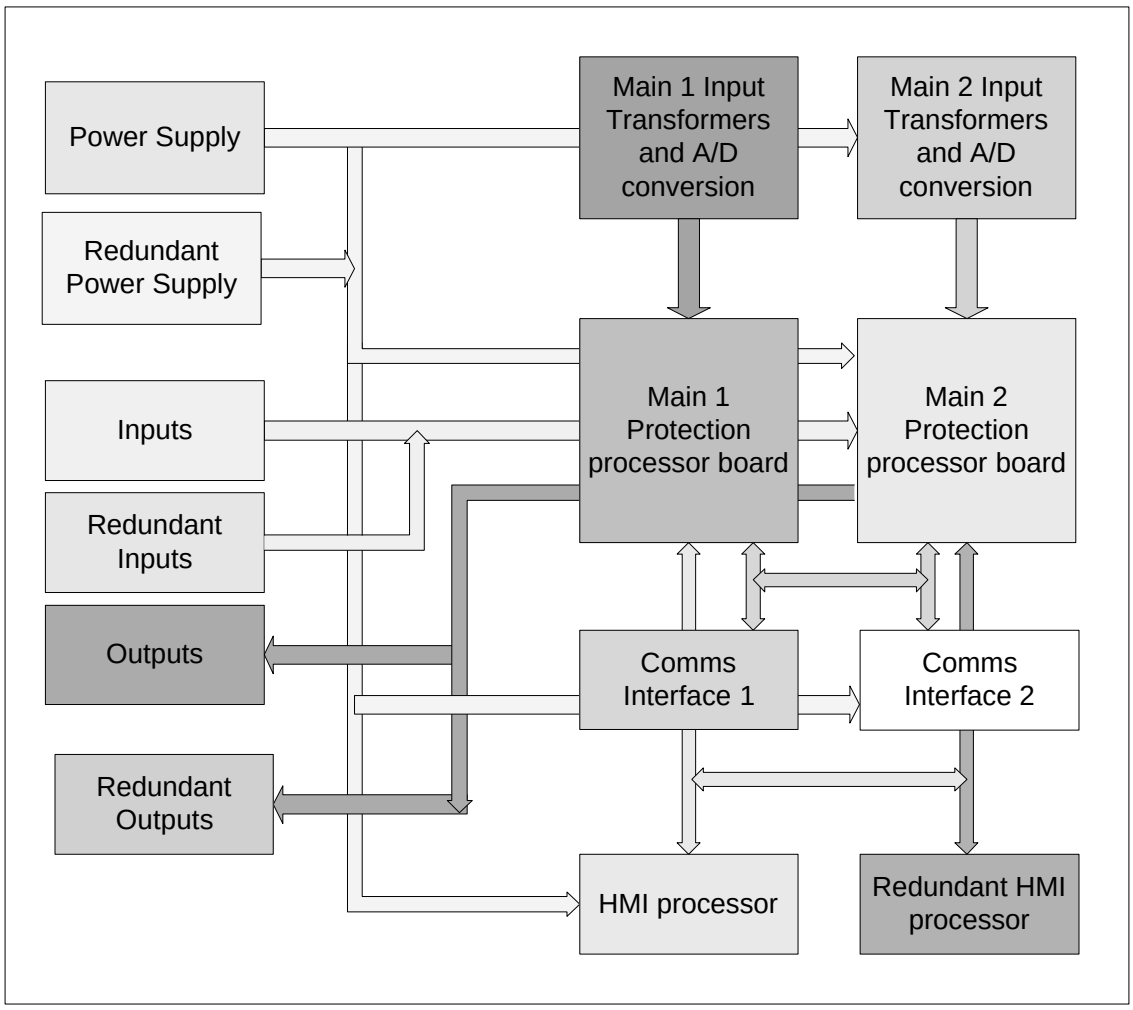

Figure 12. New redundant relay system with redundant comms interfaces

The failure rate for the new redundant System with communications is estimated in a Fault Tree:

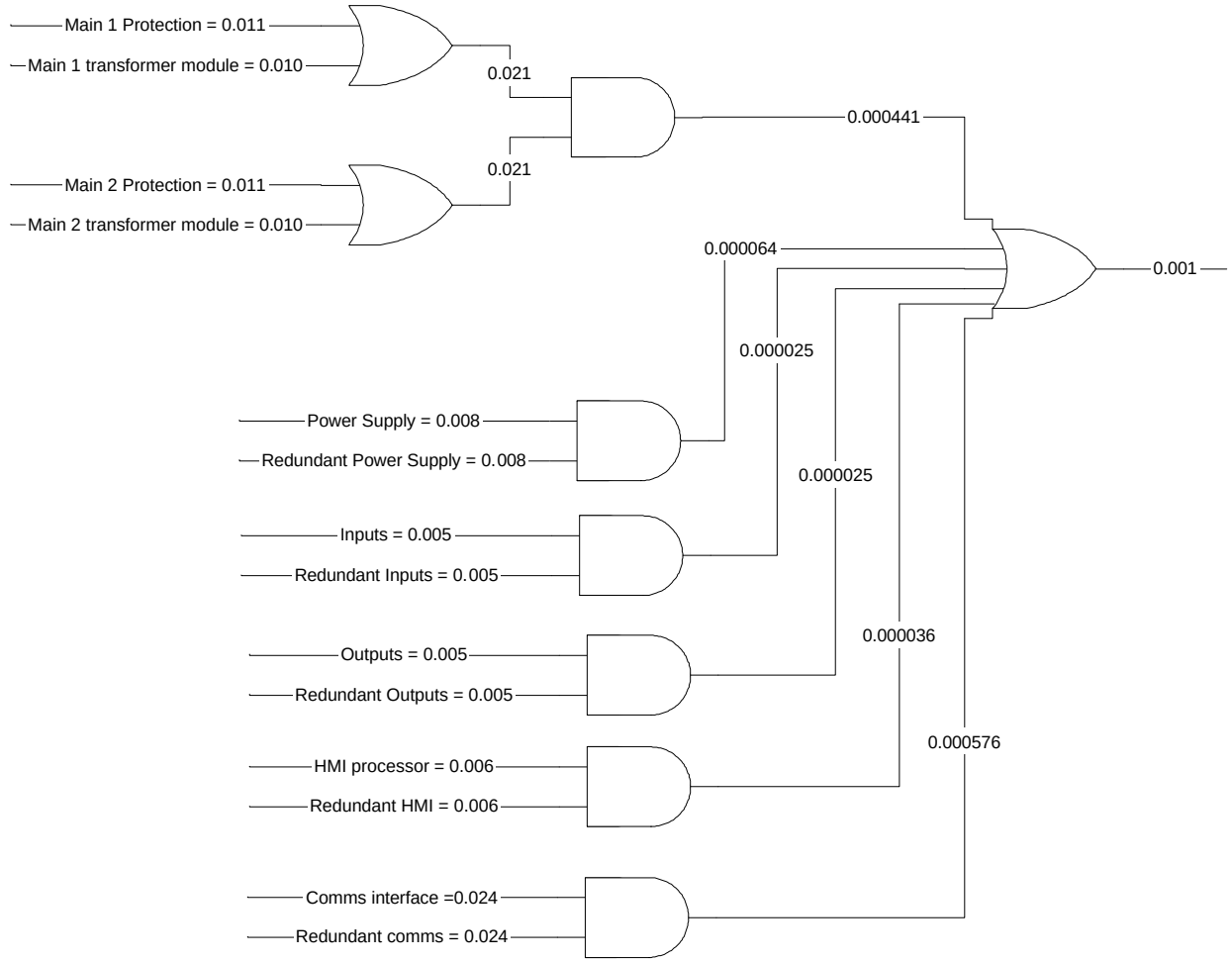

Figure 13. Fault Tree for the new redundant system with redundant comms

Summarizing our results in a table yield the following:

System	*Failure rate per line protection (two terminals)*	*MTBF (years)*
Single relay with single channels	0.138	7
Redundant relay with redundant channel	0.019	53
New redundant relay system with redundant communications	2 x 0.001=0.002	500

Table 8.

We can see that the New System improves MTBF with a factor of 10 as compared to the conventional redundant relay system.

Redundant communications channels

We showed earlier that a redundant relay channel greatly reduces overall protection system failure rate. However, it may be costly to add communications channels. A dedicated fiber for relay-to-relay communications could be difficult to justify economically. The same fiber is capable of a much higher bandwidth and could carry much more data. A single mode fiber used for 64 or 19.2 kbps relay data could transport 9953.28 Mbps (SONET OC-192) if multiplexed. Still, a relay engineer prefers a dedicated relay-to-relay communications link whether it is fiber or some other media. We will present some examples of how a redundant channel can be achieved without requiring an additional fiber pair, if one dedicated fiber pair already is available for relaying.

Double circuit line applications

In case a single dedicated fiber is available for each primary line protection, a redundant pilot channel for a secondary protection scheme can easily be made available by using our new Protective Relay and Communications System with 'pass-through' functionality.

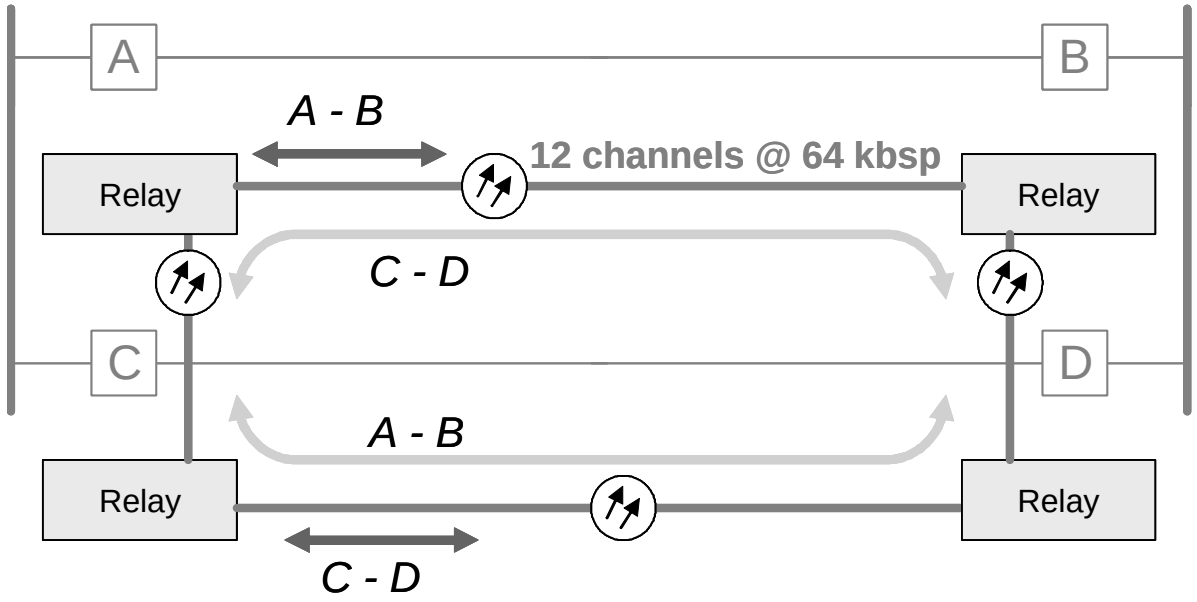

Figure 14. Redundant channels on single fiber pairs on a double circuit line

The protection for line A-B communicates in conventional manner over a fiber pair from terminal A to terminal B. In addition, the relay at A passes its information via another comms port to the C terminal relay in the same substation. The C relay does not use this data and just embeds the information into the data stream to be sent to terminal D; it provides a 'pass-through' operation. When the data is received at terminal D, the relay at D delivers it to terminal B. Consequently, the protection for line A-B has two alternative paths for relay-to-relay communications; directly between A and B, or from A via C and D to B.

The ‘Relay’ shown in Figure 14 can be a Current Differential Relay, a Distance Protection, or both. The ‘Relay’ also includes logic for teleprotection signaling.

While multiplexing is taking place, it is transparent to the relays. For all practical purposes, the relays still have a direct point-to-point connection. The ‘pass-through’ function is transporting incoming data from one communications interface directly to another channel on another communications interface. As no processing of the data is taking place, the ‘pass-through’ is made without any significant delay (<250 microseconds). Data communications remains synchronous during the pass-through process and can be used for most current differential relay channels, teleprotection channels and distance protection pilot communications.

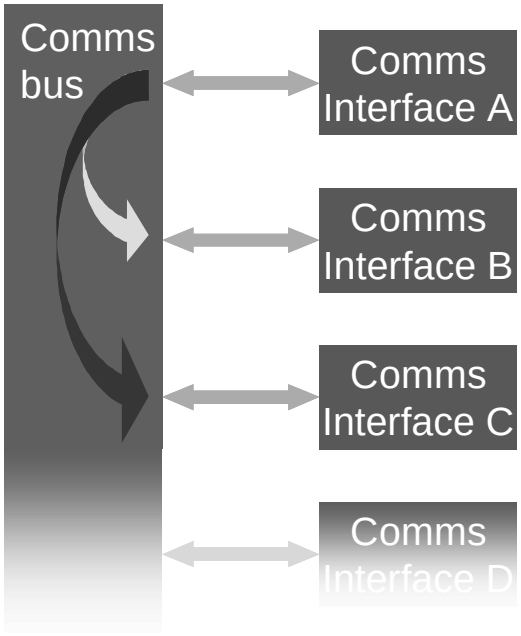

Figure 15. Pass-through functionality

Three-terminal line applications

The new relay system can provide redundant communication paths on three-terminal line applications as well. If a fiber pair already exists between each line terminal, this is accomplished without any additional comms interfaces. The pass-through function is using the same comms heads as the direct communication path. Similar to the double-line application, we can see that data from A to B is sent both directly from A to B and on the redundant channel from A to C to B.

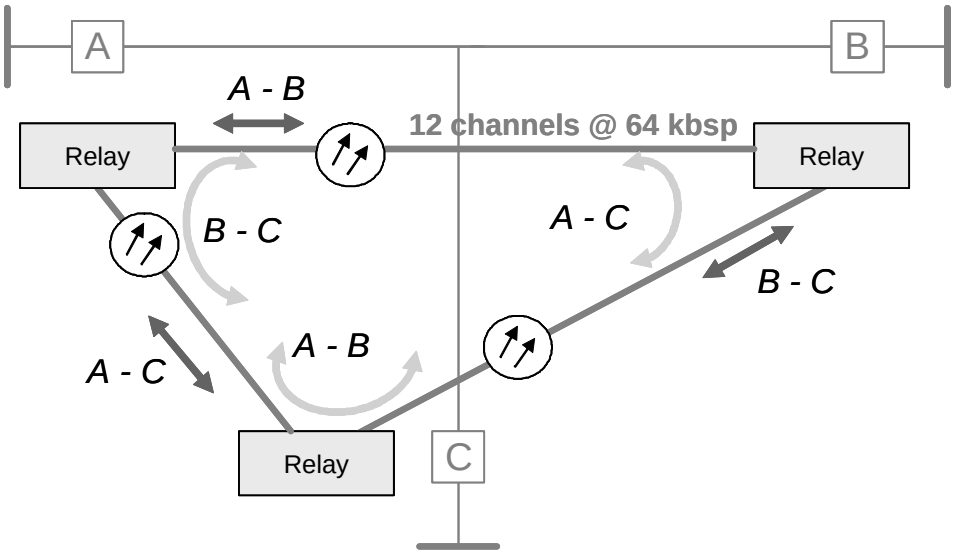

Figure 16. Three terminal line application

Existing dedicated fiber installations

In addition to using the built-in relay functions, existing dedicated fiber links can be routed through the new Protective Relaying and Communications System using any of the twelve 64 kbps channels available for relaying. These channels can be used for secure and dependable transfer trip or high speed pilot communications for current differential or distance protection.

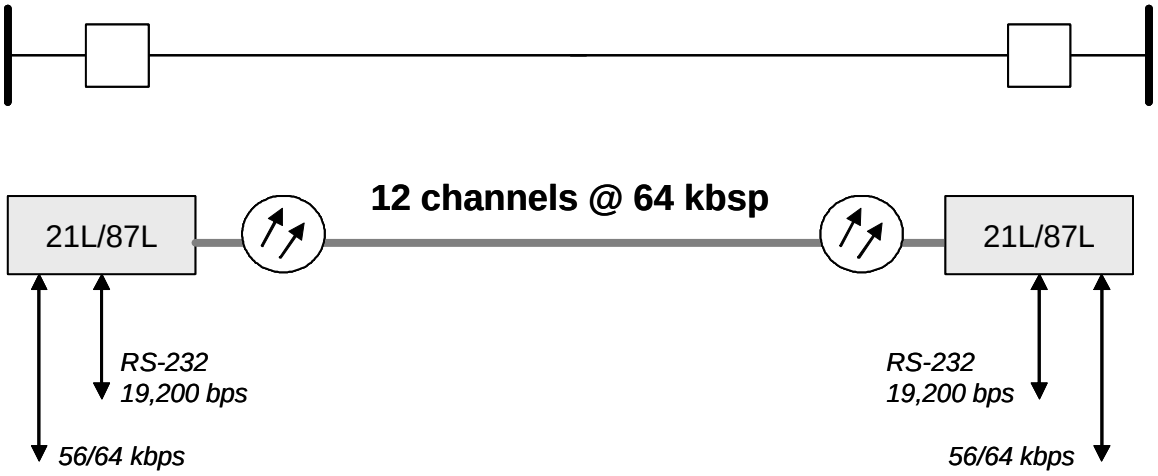

Figure 17. Optimizing existing fiber installation

No changes of the existing scheme are required. A protection with low-speed RS-232 communication or current differential relays using 64 kbps over fiber will still have the use of a functionally dedicated point-to-point connection.

System overview

The new protective relay and communications system is a device built-up of independent functional modules. Protective devices such as line distance protection, current differential protection and teleprotection are applied with selected redundancy. These devices share common modules, such as power supply, main processor, input/output boards and comms interfaces. All common modules can be applied with redundancy and as previously shown, the resultant overall system redundancy is higher than what is accomplished by completely separate redundant systems.

The new system is truly modular and functional modules can be added at any time as needed. Input and output contact boards and comms interface modules are freely selectable to suit the application, and the required degree of redundancy.

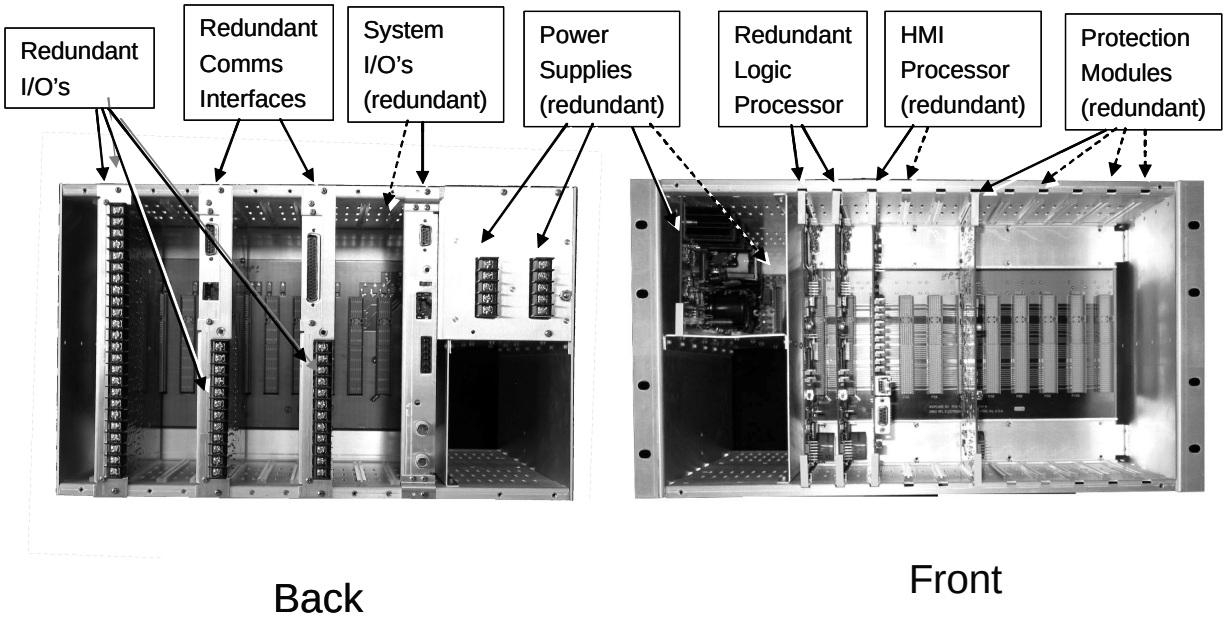

Figure 18. System design

Maintenance issues have not been forgotten in the design of the new system. Again, borrowing solutions from the telecomms industry, all modules are hot-swappable. This means that one protection system can be taken out of service for testing without affecting a second system that will continue to protect the line.

This paper has focused on dedicated fiber optic communications channel applications. However, the system can use any available communication media for pilot and teleprotection communications. Conventional voice channels or Power Line Carrier can be used in combination with digital media, operating in parallel or as redundant, back-up paths.

Conclusions

- Reliability is a measure on how well a protective relay system will perform and is a combination of security and dependability. Added redundancy greatly improves dependability.
- While the redundancy calculation examples in this paper have been based on a conservative part count, they are still useful to illustrate the relative difference between the redundant configurations. The examples clearly show that a higher degree of redundancy is achieved by the approach applied in the new system presented.
- The new redundant system improves failure rates by a factor of 10 as compared to a conventional redundant relay and communications system.
- Redundant channels can be accomplished over a single fiber pair without losing the functional point-to-point characteristics of the pilot relaying communications channel.
- The new Protective Relay and Communications System satisfies stringent redundancy requirements in a cost efficient way, providing an economical and simple method of improving protection system reliability.

References

[1] The IEEE Standard Dictionary of Electrical and Electronics Terms, IEEE Std 100-1996

[2] Transmission Protective Relay System Performance Measuring Methodology IEEE/PSRC Working Group I3, 9/16/1999.

[3] IEC 60834-1, 1999-10. Teleprotection equipment of power systems – Performance and testing.

[4] Reliability Analysis of Transmission protection Using Fault Tree Methods, E. O. Schweitzer III, et. al. www.selinc.com

Improve Your Protection Quality by Mining Historical Microprocessor Relay Data, Lawrence C. Gross, Jr., Scott L. Hayes, 28th Annual Western Protective Relay Conference, 2001.

Protective Relaying Theory and Applications, Second Edition, Walter A. Elmore, 2004

Biography

Solveig M. Ward
Solveig received her M.S.E.E. from the Royal Institute of Technology, Sweden in 1977. The same year she joined ABB Relays. She has held many positions in Marketing, Application, and Product Management. Assignments include a six-month period in Montreal, Canada and two years in Mexico. When Ms. Ward returned to Sweden, she was responsible for the application aspects in the development of a numerical distance protection relay and in charge of marketing the product. After transferring to ABB in the US 1992, she was involved in numerical distance protection application design, and was Product Manager for ABB's line of current differential and phase comparison relays.
Solveig has written, co-authored and presented several technical papers at Protective Relaying Conferences. She is a member of IEEE and holds one patent, "High Speed Single Pole Trip Logic".
In 2002, Solveig joined RFL Electronics Inc. as Director of Product Marketing. She is presently involved in the development of new products.

Tom Dahlin
Tom has spent 23 years with RFL Electronics Inc. after graduating from Metropolitan Technical Institute. Tom has held numerous positions at RFL in Final Test, Customer Service, R & D Engineering, Systems Engineering and most recently in Sales as an Engineer and now Director of Sales. Tom spent many years working with Protective Relaying and teleprotection before changing his focus to telecommunications. Today, Tom spends most of his time designing SONET/SDH networks for Utility applications. Tom is an active member of the IEEE and resides on several working groups under the Power Systems Communications Committee including the "SONET and ATM Committee for Electric Utilities".

William G. Highinbotham
Bill has been Vice President of RFL Electronics Inc. Research and Development Engineering group since 1994. He joined RFL 14 years ago as a senior design engineer. In this period he has been involved in the development of numerous RFL products in the areas of communications and protection. Bill is active in the IEEE Power Systems Relaying Committee and is currently chairman of the working group revising the "IEEE Guide for Power System Protective Relay Applications of Audio Tones over Voice Grade Channels". Bill received his BSEE from Rutgers University in 1984 and worked in the biomedical engineering field for 5 years.